CRIMINAL JUSTICE CONNECTIONS

An employee publication of the Texas Department of Criminal Justice

March/April 2013
Volume 20 Issue 4

Policies and Benefits

Information Security: best practices in computer passwords

In our high tech, computerized world, it seems like a password is required for everything we do. Keeping all these passwords secure can be difficult, but a weak password – even if it's easy to remember – makes it easy for hackers to the gain unauthorized access to our data systems. A strong password improves security and reduces the likelihood that critical information will be compromised.

Keeping up with password security requirements can be challenging, and sometimes it's easy to forget why they are so important. We might think that the data on our computers is not so significant that anyone would make the effort to hack the account, but a compromised computer can allow unauthorized users access to Texas Department of Criminal Justice (TDCJ) information. Maintaining password security is sometimes inconvenient, but these practices are in place to protect you, the network and the agency.

Sharing Passwords

Your account is more likely to be compromised by someone you know rather than an anonymous hacker, so keep your usernames and passwords secret. An unauthorized user can send out e-mails, launch attacks and even commit a variety of crimes, all of which would be traced back to your user ID. The easiest way to avoid this situation is to simply use strong passwords and do not tell anyone your password, or allow them to log in under your account.

Never write down your passwords or share them with coworkers. If you need help, write down a hint to remind you of the word, but never write down the password itself. Store the hint in a safe place away from your computer. If you suspect that your account has been compromised, report it to your supervisor and immediately change your password.

Long Passwords = Strong Passwords

The longer the password, the harder it is to guess, so make your passwords long and use mixed-case (upper and lowercase) letters and numbers. It's tempting to use a common word, username, or even the name of a pet or family member. While this makes it easy to remember, it significantly increases the chances that the password will be compromised.

Using numbers, symbols, and mixed-case letters increases the number of possible variations, making your password more difficult to guess. If you use letters and numbers, the number of possible 10-character passwords is practically inexhaustible, so you won't run out of new combinations.

Using Paraphrases

One way to create strong, easy-to-remember passwords is to use a passphrase rather than a normal word. An example of a good passphrase is: $t4rWaRs (Star Wars). While this looks like a word or phrase, a hacker's program would take much more time to discover this password because of the upper and lowercase characters, special characters and numbers.

Continued on page 2

March/April 2013
Volume 20 Issue 4

Continued from page 1

Lock Your Computer

We all have to step away from our computer sometimes, whether it's to go to lunch, the bathroom, or even just to stretch our legs for a bit. In those few minutes away, a malicious user can install harmful software which can easily track your user names and passwords. Your computer account can then be used to launch an attack, or to gather information, and it can be difficult for you to prove that you were not the person logged in and breaking security policy. To lock your computer, just remember the phrase: If you're out of your seat: Control-Alt-Delete.

If you have questions, comments or suggestions regarding information security, you can send an e-mail to TDCJ's Information Security Office at iso@tdcj.state.tx.us, or call them at 936-437-1800.●